

# On BEL-configurations and finite semifields

Michel Lavrauw and John Sheekey

February 12, 2014

## Abstract

The BEL-construction for finite semifields was introduced in [3]; a geometric method for constructing semifield spreads, using so-called BEL-configurations in  $V(rn, q)$ . In this paper we investigate this construction in greater detail, and determine an explicit multiplication for the semifield associated with a BEL-configuration in  $V(rn, q)$ , extending the results from [3], where this was obtained only for  $r = n$ . Given a BEL-configuration with associated semifields spread  $\mathcal{S}$ , we also show how to find a BEL-configuration corresponding to the dual spread  $\mathcal{S}^d$ . Furthermore, we study the effect of polarities in  $V(rn, q)$  on BEL-configurations, leading to a characterisation of BEL-configurations associated to symplectic semifields.

We give precise conditions for when two BEL-configurations in  $V(n^2, q)$  define isotopic semifields. We define operations which preserve the BEL property, and show how non-isotopic semifields can be equivalent under this operation. We also define an extension of the “switching” operation on BEL-configurations in  $V(2n, q)$  introduced in [3], which, together with the transpose operation, leads to a group of order 8 acting on BEL-configurations.

1

## 1 Introduction

A finite semifield  $(\mathbb{S}, +, \circ)$  is a finite division algebra except that associativity of multiplication is not assumed. Precisely:  $(\mathbb{S}, +)$  is an abelian group; both distributive laws hold;  $(\mathbb{S}, \circ)$  has no zero divisors and has an identity. If we do not assume a multiplicative identity element, the structure is known as a presemifield. When there is no confusion possible, we will just write  $\mathbb{S}$  instead of  $(\mathbb{S}, +, \circ)$ , and we will conveniently choose between the notations  $\mathbb{S}(x, y)$  and  $x \circ y$  for the multiplication of two elements  $x, y \in \mathbb{S}$ .

---

<sup>1</sup>MSC: 12K10, 17A35, 51A40, 51A35.

Keywords: Finite semifield; Spread; BEL-configuration.

The first proper finite semifields were constructed by Dickson in 1906. Albert defined an important class of semifields known as generalized twisted fields. Semifields play a key role in the study of projective planes, as they correspond to translation planes which are also dual translation planes, and they are also related to various other structures from finite geometry and the theory of finite fields. For more background, history, and known classifications, see for example [10], [8], [15] and [14]. Most of the remainder of this section is standard knowledge in the subject, but we reproduce it here for clarity of exposition and to establish notation and conventions.

To each semifield there are several important substructures, all of which are isomorphic to finite fields. The *left nucleus*  $N_l(\mathbb{S})$ , the *middle nucleus*  $N_m(\mathbb{S})$ , and the *right nucleus*  $N_r(\mathbb{S})$  are defined as follows:

$$\begin{aligned} N_l(\mathbb{S}) &:= \{x : x \in \mathbb{S} \mid x \circ (y \circ z) = (x \circ y) \circ z, \forall y, z \in \mathbb{S}\}, \\ N_m(\mathbb{S}) &:= \{y : y \in \mathbb{S} \mid x \circ (y \circ z) = (x \circ y) \circ z, \forall x, z \in \mathbb{S}\}, \\ N_r(\mathbb{S}) &:= \{z : z \in \mathbb{S} \mid x \circ (y \circ z) = (x \circ y) \circ z, \forall x, y \in \mathbb{S}\}. \end{aligned}$$

The intersection  $N(\mathbb{S})$  of the nuclei is called the associative centre, and the elements of  $N(\mathbb{S})$  which commute with all other elements of  $\mathbb{S}$  form the centre  $Z(\mathbb{S})$ . Then  $\mathbb{S}$  has the structure of a left vector space over  $N_l(\mathbb{S})$ , which we may denote by  $V_l(\mathbb{S})$ . Similarly  $\mathbb{S}$  has the structure of a left and right vector space over  $N_m(\mathbb{S})$ , and a right vector space over  $N_r(\mathbb{S})$ .

Let  $\mathbb{S}$  be an  $n$ -dimensional semifield over  $\mathbb{F}_q$ , i.e. a semifield of order  $q^n$  with centre containing  $\mathbb{F}_q$ . We identify the elements of  $\mathbb{S}$  with the elements of  $\mathbb{F}_{q^n}$ . It follows from the definition that there exist unique elements  $c_{ij} \in \mathbb{F}_{q^n}$  such that

$$\mathbb{S}(x, y) = \sum_{i,j=0}^{n-1} c_{ij} x^{q^i} y^{q^j}.$$

For example, Albert's generalized twisted fields are defined as follows. Let  $\alpha, \beta \in \text{Aut}(\mathbb{F}_{q^n} : \mathbb{F}_q)$ , and  $c \in \mathbb{F}_{q^n}$  such that  $c \notin \{x^{\alpha-1}y^{\beta-1} : x, y \in \mathbb{F}_{q^n}\}$ . Then the multiplication on  $\mathbb{F}_{q^n}$

$$x \circ y = xy - cx^\alpha y^\beta$$

defines a presemifield of order  $q^n$ . We will denote this presemifield by  $\text{GTF}_{c,\alpha,\beta}$ . If  $x^\alpha = x^{q^k}$  and  $y^\beta = y^{q^m}$ , we see that

$$c_{ij} = \begin{cases} 1 & \text{if } i = j = 0, \\ -c & \text{if } i = k, j = m, \\ 0 & \text{otherwise.} \end{cases}$$

Continuing with the semifield  $\mathbb{S}$  as before we have that each  $y \in \mathbb{S}$  defines an  $\mathbb{F}_q$ -endomorphism of  $\mathbb{S}$ , denoted by  $R_y$ , defined by

$$R_y(x) := \mathbb{S}(x, y). \tag{1}$$

We call this the endomorphism of right multiplication by  $y$ . Since  $\mathbb{S}$  has no zero divisors,  $R_y$  is nonsingular for each  $y \neq 0$ , and the set  $R(\mathbb{S}) := \{R_y : y \in \mathbb{S}\}$  is an  $\mathbb{F}_q$ -subspace of  $\mathbb{F}_q$ -endomorphisms of  $\mathbb{S}$ , where each nonzero element is nonsingular. We call  $R(\mathbb{S})$  the spread set of  $\mathbb{S}$ .

Similarly we can define the endomorphisms of left multiplication

$$L_x(y) := \mathbb{S}(x, y).$$

If we define  $r_i(y) = \sum_j c_{ij} y^{q^j}$ , and  $l_j(x) = \sum_i c_{ij} x^{q^i}$ , then we have that

$$R_y(x) = \sum_i \left( \sum_j c_{ij} y^{q^j} \right) x^{q^i} = \sum_i r_i(y) x^{q^i}; \quad (2)$$

$$L_x(y) = \sum_j \left( \sum_i c_{ij} x^{q^i} \right) y^{q^j} = \sum_j l_j(x) y^{q^j}. \quad (3)$$

An  $n$ -spread  $\mathcal{S}$  in  $V(rn, q)$  is a set of subspaces of dimension  $n$  which pairwise intersect trivially, and which partition the nonzero elements of  $V(rn, q)$ . It is well known that every (pre)semifield defines a spread in the following way. We represent the elements of  $V(2n, q)$  by elements of  $\mathbb{S}^2$ . Then for each  $y \in \mathbb{S}$ , we define

$$A_y := \{(x, \mathbb{S}(x, y)) : x \in \mathbb{S}\} = \{(x, R_y(x)) : x \in \mathbb{S}\}.$$

We also define

$$A_\infty = \{(0, x) : x \in \mathbb{S}\}.$$

Then the set of subspaces of dimension  $n$

$$\mathcal{S}(\mathbb{S}) := \{A_y : y \in \mathbb{S}\} \cup \{A_\infty\} \quad (4)$$

defines a spread.

Conversely, every semifield spread defines a (pre)semifield. A spread  $\mathcal{S}$  is a semifield spread if there exists some element  $T \in \mathcal{S}$ , and a group  $G \leq \Gamma L(2n, q)$  fixing  $T$  pointwise and acting transitively on the other elements of  $\mathcal{S}$ . Note that in the spread  $\mathcal{S}(\mathbb{S})$  the special element is  $A_\infty$ .

Two semifields  $\mathbb{S}$  and  $\mathbb{S}'$  are isotopic if there exist nonsingular linear maps  $A, B, C : \mathbb{S} \rightarrow \mathbb{S}'$  such that

$$\mathbb{S}'(A(x), B(y)) = C(\mathbb{S}(x, y))$$

for all  $x, y \in \mathbb{S}$ . We denote the isotopy class of  $\mathbb{S}$  by  $[\mathbb{S}]$ .

A well known result of Albert [1] says that two (pre)semifields are isotopic if and only if the spreads they define are equivalent (under the action of  $\Gamma L(2n, q)$ ). For equivalent spreads  $\mathcal{S}_1$  and  $\mathcal{S}_2$  we write  $\mathcal{S}_1 \simeq \mathcal{S}_2$ .

It was shown in [10] that from each (pre)semifield, we can obtain a chain of (up to) six isotopy classes, which we call the Knuth orbit and denote by  $\mathcal{K}(\mathbb{S})$ . These

are obtained via an action of the symmetric group  $S_3$  on the set of isotopism classes of semifields, generated by the two operations dual, denoted by  $[\mathbb{S}]^d$ , and transpose, denoted by  $[\mathbb{S}]^t$ .

The action of  $S_3$  in [10] was defined using the cubical array of the structure constants of the semifield, but here we give the alternative more geometric definition of the Knuth orbit. The dual of  $[\mathbb{S}]$  corresponds to the dual projective plane and the opposite algebra  $\mathbb{S}^d$ , that is

$$\mathbb{S}^d(x, y) = \mathbb{S}(y, x)$$

and  $[\mathbb{S}]^d := [\mathbb{S}^d]$ . The transpose  $[\mathbb{S}]^t$  of  $[\mathbb{S}]$  can be defined using the spread  $\mathcal{S}(\mathbb{S})$ , and corresponds to the dual spread with respect to some nondegenerate symmetric bilinear form on  $V(2n, q)$ . Note that different choices of forms give equivalent spreads. The spread set of  $[\mathbb{S}]^t$  then consists of the adjoint linear transformations with respect to some nondegenerate symmetric bilinear form on  $V(n, q)$ . For a particular choice of form and basis, this adjoint becomes the transpose operation on matrices, which explains the notation and the name. See for example [10] for this. Here we will choose a different form, which better suits our needs for this paper.

We define the form  $b_\epsilon$  on  $V(2n, q)$  by

$$b_\epsilon((a, b), (c, d)) = \text{tr}(ad - bc), \quad (5)$$

where  $\text{tr}$  denotes the trace function from  $\mathbb{F}_{q^n}$  to  $\mathbb{F}_q$ , that is

$$\text{tr}(x) = x + x^q + \dots + x^{q^{n-1}}.$$

Given a subspace  $M$ , define the dual of  $M$ , denoted by  $M^\epsilon$ , by

$$M^\epsilon = \{v : v \in V(2n, q) \mid b_\epsilon(u, v) = 0 \ \forall u \in M\}. \quad (6)$$

Let  $f$  be an  $\mathbb{F}_q$ -endomorphism of  $\mathbb{F}_{q^n}$ . It is well known that

$$f(x) = \sum_{i=0}^{n-1} f_i x^{q^i}$$

for some unique  $f_i \in \mathbb{F}_{q^n}$ . We denote by  $\hat{f}$  the adjoint of  $f$  with respect to the nondegenerate symmetric bilinear form on  $V(n, q)$  defined by

$$(x, y) \mapsto \text{tr}(xy).$$

That is,  $\hat{f}$  is the unique endomorphism such that

$$\text{tr}(f(x)y) = \text{tr}(x\hat{f}(y))$$

for all  $x, y \in \mathbb{F}_{q^n}$ . Then we have that

$$\hat{f}(x) = \sum_{i=0}^{n-1} f_{n-i}^{q^i} x^{q^i}.$$

It is not difficult to see that  $\hat{\hat{f}} = f$ , and  $\widehat{fg} = \hat{g}\hat{f}$  for all endomorphisms  $f, g$ .

The isotopism class  $[\mathbb{S}]^t$  corresponds to the dual spread of  $\mathcal{S}(\mathbb{S})$ , that is  $\mathcal{S}(\mathbb{S})^\epsilon = \{T^\epsilon : T \in \mathcal{S}(\mathbb{S})\}$ . Note that  $A_\infty^\epsilon = A_\infty$ .

Now we can see that

$$A_y^\epsilon = \{(x, \hat{R}_y(x)) : x \in \mathbb{F}_{q^n}\},$$

since

$$\begin{aligned} b_\epsilon((x, R_y(x)), (z, \hat{R}_y(z))) &= \text{tr}(x\hat{R}_y(z) - R_y(x)z) \\ &= \text{tr}(z(R_y(x) - R_y(x))) \\ &= 0 \end{aligned}$$

for all  $x, z \in \mathbb{F}_{q^n}$ .

This allows us to define the transpose of  $[\mathbb{S}]$  directly from the multiplication  $\mathbb{S}(x, y)$ . We have shown the following.

**Lemma 1.** *Let  $\mathbb{S}$  be a semifield. Then  $[\mathbb{S}]^t = [\mathbb{S}^t]$  where*

$$\mathbb{S}^t(x, y) := \hat{R}_y(x) = \sum_i (r_{n-i}(y))^{q^i} x^{q^i}, \quad (7)$$

where  $R_y$  and  $r_i$  are as defined in (1) and (2).

In [10] Knuth also showed that these operations are well defined up to isotopism. This fact is easily verified using the geometric description of the transpose and dual operations given above, and goes as follows.

Suppose  $\mathbb{S}$  is isotopic to  $\mathbb{S}'$ , i.e. there exist a triple of invertible linear transformations  $(A, B, C)$  such that  $\mathbb{S}'(A(x), B(y)) = C(\mathbb{S}(x, y))$  for all  $x, y \in \mathbb{S}$ . Then

$$C(\mathbb{S}^d(x, y)) = C(\mathbb{S}(y, x)) = \mathbb{S}'(A(y), B(x)) = \mathbb{S}'^d(B(x), A(y)),$$

and hence  $\mathbb{S}^d$  is isotopic to  $\mathbb{S}'^d$ , with corresponding isotopism  $(B, A, C)$ .

Now  $CR_y(x) = C(\mathbb{S}(x, y)) = \mathbb{S}'(A(x), B(y)) = R'_{B(y)}A(x)$  for all  $x, y \in \mathbb{S}$ , and hence  $CR_y = R'_{B(y)}A$  for all  $y \in \mathbb{S}$ . Taking the adjoint of both sides, we get  $\hat{R}_y\hat{C} = \hat{A}\hat{R}'_{B(y)}$ . Hence

$$\hat{A}^{-1}(\mathbb{S}^t(x, y)) = \hat{A}^{-1}\hat{R}_y(x) = \hat{R}'_{B(y)}\hat{C}^{-1}(x) = \mathbb{S}'^t(\hat{C}^{-1}(x), B(y)),$$

implying that  $\mathbb{S}^t$  is isotopic to  $\mathbb{S}'^t$ , as claimed. The corresponding isotopism is  $(\hat{C}^{-1}, B, \hat{A}^{-1})$ .

It is clear from the above that these two operations satisfy  $t^2 = d^2 = \text{id}$ ,  $tdt = dtd$ , and so form a group isomorphic to the symmetric group  $S_3$ . Hence we get a chain of (up to) 6 isotopism classes. The set of these isotopism classes is called the Knuth orbit of a semifield  $\mathbb{S}$ :

$$\mathcal{K}(\mathbb{S}) = \{[\mathbb{S}], [\mathbb{S}^t], [\mathbb{S}^d], [\mathbb{S}^{td}], [\mathbb{S}^{dt}], [\mathbb{S}^{ttd}] = [\mathbb{S}^{dtd}]\}. \quad (8)$$

We summarise a multiplication for each isotopism class in the Knuth orbit of  $\mathbb{S}$  in the below table. We give two equivalent expressions for convenience. Here indices such as  $-i$  are understood to be modulo  $n$ , and all sums are understood to be over all  $i, j \in \{0, \dots, n-1\}$ .

$\mathbb{S}$	$\sum c_{ij} x^{q^i} y^{q^j}$	$\sum c_{ij} x^{q^i} y^{q^j}$
$\mathbb{S}^t$	$\sum c_{-i, i-j}^q x^{q^i} y^{q^j}$	$\sum c_{ij}^{q^{-i}} x^{q^{-i}} y^{q^{j-i}}$
$\mathbb{S}^d$	$\sum c_{ji} x^{q^i} y^{q^j}$	$\sum c_{ij} x^{q^j} y^{q^i}$
$\mathbb{S}^{td}$	$\sum c_{-j, j-i}^{q^j} x^{q^i} y^{q^j}$	$\sum c_{ij}^{q^{-i}} x^{q^{j-i}} y^{q^{-i}}$
$\mathbb{S}^{dt}$	$\sum c_{j-i, -i}^{q^i} x^{q^i} y^{q^j}$	$\sum c_{ij}^{q^{-j}} x^{q^{-j}} y^{q^{i-j}}$
$\mathbb{S}^{dtd}$	$\sum c_{i-j, -j}^{q^j} x^{q^i} y^{q^j}$	$\sum c_{ij}^{q^{-j}} x^{q^{i-j}} y^{q^{-j}}$

**Example 1.** If  $\mathbb{S} = \text{GTF}_{c, \alpha, \beta}$ , then the Knuth orbit is represented in the following table.

	Multiplication	GTF
$\mathbb{S}$	$xy - cx^\alpha y^\beta$	$(c, \alpha, \beta)$
$\mathbb{S}^t$	$xy - c^{1/\alpha} x^{1/\alpha} y^{\beta/\alpha}$	$(c^{1/\alpha}, 1/\alpha, \beta/\alpha)$
$\mathbb{S}^d$	$xy - cx^\beta y^\alpha$	$(c, \beta, \alpha)$
$\mathbb{S}^{td}$	$xy - c^{1/\alpha} x^{\beta/\alpha} y^{1/\alpha}$	$(c^{1/\alpha}, \beta/\alpha, 1/\alpha)$
$\mathbb{S}^{dt}$	$xy - c^{1/\beta} x^{1/\beta} y^{\alpha/\beta}$	$(c^{1/\beta}, 1/\beta, \alpha/\beta)$
$\mathbb{S}^{dtd}$	$xy - c^{1/\beta} x^{\alpha/\beta} y^{1/\beta}$	$(c^{1/\beta}, \alpha/\beta, 1/\beta)$

In [4], the question of when two generalized twisted fields are isotopic was answered. We state this result here, as we will need it in later sections.

**Theorem 1** ([4]). *The semifields  $\text{GTF}_{c, \alpha, \beta}$  and  $\text{GTF}_{c', \alpha', \beta'}$  are isotopic if and only if either*

(i)  $\alpha = \alpha', \beta = \beta'$  and  $c^\rho = c' a^{1-\alpha} b^{1-\beta}$  for some  $\rho \in \text{Aut}(\mathbb{F}_{q^n})$ ,  $a, b \in \mathbb{F}_{q^n}^*$ ,  
or

(ii)  $\alpha' = 1/\alpha, \beta' = 1/\beta$  and  $c'^\rho = c^{-1} a^{1-\alpha} b^{1-\beta}$ , for some  $\rho \in \text{Aut}(\mathbb{F}_{q^n})$ ,  
 $a, b \in \mathbb{F}_{q^n}^*$ .

## 2 BEL-construction

The concept of a BEL-configuration was introduced in [3], and further developed in [12] and [13]. In this section we will recall the definition, and how a BEL-configuration can be used to construct of a semifield spread. We restrict ourselves to BEL-configurations where both subspaces  $U$  and  $W$  are subspaces as in the original paper [3], and will not consider the generalization [13] to linear

sets. We obtain an explicit formula for the pre-semifield multiplication obtained from a BEL-configuration in  $V(rn, q)$ .

For a spread  $\mathcal{D}$  and a subset  $A$  of a vector space  $V$ , we define the sets

$$\begin{aligned}\mathcal{B}_{\mathcal{D}}(A) &= \{S \in \mathcal{D} \mid S \cap A \neq \{0\}\}; \\ \tilde{\mathcal{B}}_{\mathcal{D}}(A) &= \bigcup_{S \in \mathcal{B}(A)} \{x : x \in S^\times\}.\end{aligned}$$

That is,  $\mathcal{B}_{\mathcal{D}}(A)$  is the set of elements of  $\mathcal{D}$  intersecting  $A$  nontrivially, and  $\tilde{\mathcal{B}}_{\mathcal{D}}(A)$  is the set of nonzero vectors contained in those elements. We will omit the subscript  $\mathcal{D}$  whenever there is no ambiguity. If  $0 \neq v \in V$ , we denote by  $\mathcal{B}_{\mathcal{D}}(v)$  the unique element of  $\mathcal{D}$  containing  $v$ . Then by definition,  $\mathcal{D} = \{\mathcal{B}_{\mathcal{D}}(v) : v \in V^\times\}$ .

A Desarguesian spread is a spread obtained by field reduction, see e.g. [17].

**Definition 1.** A BEL-configuration in  $V(rn, q)$  is a triple  $(\mathcal{D}, U, W)$  such that:

- $\mathcal{D}$  is a Desarguesian  $n$ -spread;
- $U$  is a subspace of dimension  $n$ ;
- $W$  is a subspace of dimension  $rn - n$ ;
- $\mathcal{B}(U) \cap \mathcal{B}(W) = \emptyset$ .

We now choose a specific Desarguesian spread  $\mathcal{D}_{r,n,q}$ , which we will consider fixed for the remainder of this paper. We represent elements of  $V(rn, q)$  by elements of  $(\mathbb{F}_{q^n})^r$ .

For a vector  $v = (v_1, \dots, v_r) \neq 0$ ,  $v_i \in \mathbb{F}_{q^n}$ , we define the vector subspace  $\mathcal{B}(v)$  of dimension  $n$  in  $V(rn, q)$  as follows:

$$\mathcal{B}(v) := \{(\alpha v_1, \alpha v_2, \dots, \alpha v_r) : \alpha \in \mathbb{F}_{q^n}\} \leq V(rn, q).$$

We then take the set of all such subspaces  $\mathcal{D}_{r,n,q} = \{\mathcal{B}(v) : v \in V^\times\}$ , which forms a Desarguesian spread. We will omit the subscripts when there is no ambiguity. Obtaining a spread in this way is an example of the technique known as field reduction. See [17] for a detailed exposition of this.

The following lemma is trivial, but we write it out explicitly for future reference.

**Lemma 2.** *The following are equivalent:*

1.  $(\mathcal{D}_{r,n,q}, U, W)$  is a BEL-configuration in  $V(rn, q)$ ;
2.  $\mathcal{B}(U) \cap \mathcal{B}(W) = \emptyset$ ;
3.  $U \cap \tilde{\mathcal{B}}(W) = \emptyset$ ;
4.  $W \cap \tilde{\mathcal{B}}(U) = \emptyset$ ;

5. No element of  $U^\times$  is an  $\mathbb{F}_{q^n}$ -multiple of an element of  $W^\times$ ;

We can embed  $V(rn, q)$  in  $V(rn + n, q)$  in a natural way, that is by letting  $V(rn + n, q) = \{(v_0, v_1, \dots, v_r) : v_i \in \mathbb{F}_{q^n}\}$ , and taking  $V(rn, q)$  to be the subspace of vectors with  $v_0 = 0$ . The spread  $\mathcal{D}_{r,n,q}$  naturally extends to the Desarguesian spread  $\mathcal{D}_{r+1,n,q}$  of  $V(rn + n, q)$ .

In [3], the following was shown.

**Theorem 2 (BEL-construction).** *Let  $(\mathcal{D}, U, W)$  be a BEL-configuration in  $V(rn, q) \leq V(rn + n, q)$ . Choose an element  $v$  of  $V(rn + n, q) \setminus V(rn, q)$ .*

*Then the set*

$$\mathcal{S}(\mathcal{D}, U, W) := \left\{ \frac{\langle \mathcal{B}(z), W \rangle}{W} : z \in \langle v, U \rangle \right\}$$

*is a semifield spread in  $\frac{V(rn+n,q)}{W} \cong V(2n, q)$ .*

**Remark 1.** *It is clear from the definition, as was shown in [3], that for any  $\phi \in \Gamma L(rn, q)$ , the semifield spread  $\mathcal{S}(\mathcal{D}^\phi, U^\phi, W^\phi)$  is equivalent to  $\mathcal{S}(\mathcal{D}, U, W)$ .*

*If  $\mathcal{D} = \mathcal{D}_{r,n,q}$ , then the group  $\Gamma L(r, q^n)$ , embedded naturally in  $\Gamma L(rn, q)$ , stabilizes  $\mathcal{D}$ , see e.g. [17]. Hence ([3], Theorem 2.4), if  $\phi \in \Gamma L(r, q^n)$ , then  $(\mathcal{D}, U, W)$  is a BEL-configuration if and only if  $(\mathcal{D}, U^\phi, W^\phi)$  is a BEL-configuration, the spreads  $\mathcal{S}(\mathcal{D}, U, W)$  and  $\mathcal{S}(\mathcal{D}, U^\phi, W^\phi)$  are equivalent, and the corresponding semifields are isotopic. So if we fix the Desarguesian spread  $\mathcal{D} = \mathcal{D}_{r,n,q}$ , we can define equivalence classes*

$$[U, W] := \{(U^\phi, W^\phi) : \phi \in \Gamma L(r, q^n)\}. \quad (9)$$

*We will return to these classes in the subsequent sections.*

**Definition 2.** *Two BEL-configurations  $(\mathcal{D}, U, W)$  and  $(\mathcal{D}', U', W')$  are called equivalent, notation  $(\mathcal{D}, U, W) \equiv (\mathcal{D}', U', W')$ , if and only if the spreads  $\mathcal{S}(\mathcal{D}, U, W)$  and  $\mathcal{S}(\mathcal{D}', U', W')$  are equivalent.*

We will sometimes denote this spread  $\mathcal{S}(\mathcal{D}, U, W)$  simply by  $\mathcal{S}(U, W)$ . Now we will show how to find a semifield multiplication which gives a spread equivalent to  $\mathcal{S}(U, W)$ . Such an explicit multiplication was only obtained in the case  $r = n$  in [3, Theorem 4.1], and this was done in order to prove that every semifield can be constructed from a BEL-configuration in  $V(n^2, q)$ . First we find a convenient way to express  $U$  and  $W$ .

**Lemma 3.** *Any subspace  $U$  of  $V(rn, q)$  of dimension  $n$  is equal to*

$$U_f := \{(f_1(x), f_2(x), \dots, f_r(x)) : x \in \mathbb{F}_{q^n}\} \quad (10)$$

*for some  $r$ -tuple  $f = (f_1, f_2, \dots, f_r)$  of  $\mathbb{F}_q$ -endomorphisms of  $\mathbb{F}_{q^n}$ .*

*Any subspace  $W$  of  $V(rn, q)$  of dimension  $rn - n$  is equal to*

$$W_g := \{(x_1, x_2, \dots, x_r) : x_i \in \mathbb{F}_{q^n} \mid \sum_{i=1}^r g_i(x_i) = 0\}. \quad (11)$$

*for some  $r$ -tuple  $g = (g_1, g_2, \dots, g_r)$  of  $\mathbb{F}_q$ -endomorphisms of  $\mathbb{F}_{q^n}$ .*



*Proof.* As  $\dim_{\mathbb{F}_q}(U) = \dim_{\mathbb{F}_q}(\mathbb{F}_{q^n}) = n$ ,  $U$  and  $\mathbb{F}_{q^n}$  are isomorphic as  $\mathbb{F}_q$ -vector spaces, and hence  $U$  is the image of some injective  $\mathbb{F}_q$ -linear map, say  $F$ , from  $\mathbb{F}_{q^n}$  into  $V(rn, q)$ . Let  $e_i$  be the element of  $(\mathbb{F}_{q^n})^r$  with 1 in the  $i$ -th position and zeroes everywhere else, and let  $V_i = \{\alpha e_i : \alpha \in \mathbb{F}_{q^n}\}$ . Then if we let  $f_i(x)e_i$  denote the projection of  $F(x)$  onto  $V_i$ , i.e.  $F(x) = \sum_i f_i(x)e_i$ , then  $U = U_f$ , as claimed.

Now  $\dim_{\mathbb{F}_q}(W) = rn - n$ , and so  $W$  is the kernel of some surjective map  $G$  from  $V(rn, q)$  onto  $\mathbb{F}_{q^n}$ . If we define  $g_i : \mathbb{F}_{q^n} \rightarrow \mathbb{F}_{q^n} : x \mapsto G(xe_i)$ , then for  $v = \sum_i x_i e_i$ , we obtain  $G(v) = \sum_i G(x_i e_i) = \sum_i g_i(x_i)$ , and  $W = W_g$ , as claimed.  $\square$

Note that if we denote  $fA = (f_1A, f_2A, \dots, f_rA)$  and  $Bg = (Bg_1, Bg_2, \dots, Bg_r)$  for any  $A, B \in GL(n, \mathbb{F}_q)$ , then clearly  $U_{fA} = U_f$  and  $W_{Bg} = W_g$ . Note also that for any  $r$ -tuple  $f$  (resp.  $g$ ) of endomorphisms,  $\dim(U_f) = n$  (resp.  $\dim(W_g) = rn - n$ ) if and only if the map  $F$  (resp.  $G$ ) as defined in the proof of Lemma 3 is injective (resp. surjective).

One of the steps in the BEL-construction consists of taking the quotient space of  $W$  in  $V(rn + n, q)$ , where we again assume  $V(rn, q)$  is embedded in  $V(rn + n, q)$  as before. To that extent we consider the following homomorphism  $T_g$  which will have kernel  $W_g$ . Given an  $r$ -tuple of endomorphisms  $g = (g_1, g_2, \dots, g_r)$ , define a map  $T_g : V(rn + n, q) \rightarrow V(2n, q)$  by

$$T_g(x_0, x_1, \dots, x_r) = (x_0, \sum_{i=1}^r g_i(x_i)).$$

Clearly  $W_g = \ker(T_g)$ , and  $\text{im}(T_g) = V(2n, q)$ . By the First Isomorphism Theorem for vector spaces, we have  $\frac{V(rn+n, q)}{W_g} \cong V(2n, q)$ , and we denote this isomorphism by  $\theta$ :

$$\theta : \frac{V(rn + n, q)}{W_g} \rightarrow V(2n, q) : v + W_g \mapsto T_g(v) \quad (12)$$

**Theorem 3.** Suppose  $(\mathcal{D}_{r,n,q}, U_f, W_g)$  is a BEL-configuration in  $V(rn, q)$ , for some  $r$ -tuples of endomorphisms  $f = (f_1, \dots, f_r)$ , and  $g = (g_1, \dots, g_r)$ . The semifield spread  $\mathcal{S}(\mathcal{D}_{r,n,q}, U_f, W_g)$  is equivalent to  $\mathcal{D}(\mathbb{S}_{f,g})$ , where  $\mathbb{S}_{f,g}$  is defined as the (pre)semifield with multiplication

$$\mathbb{S}_{f,g}(x, y) := \sum_{i=1}^r g_i(f_i(x)y). \quad (13)$$

*Proof.* Put  $v = (1, 0, \dots, 0) \in V(rn + n, q) \setminus V(rn, q)$ . Using the isomorphism from (12), we have that for all  $z \in \langle v, U_f \rangle$ ,

$$\left( \frac{\langle \mathcal{B}(z), W_g \rangle}{W_g} \right)^\theta = T_g(\mathcal{B}(z)),$$

and

$$\mathcal{S}(U_f, W_g) \simeq \{T_g(\mathcal{B}(z)) : z \in \langle v, U_f \rangle\}.$$

Suppose first that  $z \in \langle v, U_f \rangle \setminus U_f$ . Then we may take  $z = v + u$  for some unique  $u \in U_f$ . Hence  $z = (1, f_1(x), \dots, f_r(x))$  for some  $x \in \mathbb{F}_{q^n}$ , and so

$$\mathcal{B}(v + u) = \{(y, f_1(x)y, \dots, f_r(x)y) : y \in \mathbb{F}_{q^n}\}.$$

Now if  $z = u \in U_f$ , then

$$\mathcal{B}(u) = \{(0, f_1(x)y, \dots, f_r(x)y) : y \in \mathbb{F}_{q^n}\}.$$

Hence, for  $u \in U_f$

$$\begin{aligned} T_g(\mathcal{B}(u + v)) &= \{(y, \sum_{i=1}^r g_i(f_i(x)y) : y \in \mathbb{F}_{q^n}\} \\ T_g(\mathcal{B}(u)) &= \{(0, \sum_{i=1}^r g_i(f_i(x)y) : y \in \mathbb{F}_{q^n}\}. \end{aligned}$$

By Theorem 2, this gives a semifield spread. We can see that this is precisely equal to the spread  $\mathcal{S}(\mathbb{S}_{f,g})$ , where  $\mathbb{S}_{f,g}$  is as defined in (13), and  $\mathcal{S}(\mathbb{S}_{f,g})$  is as defined in (4).  $\square$

**Example 2.** Let  $f = (1, c^{1/\beta}\alpha/\beta)$ ,  $g = (1, -\beta)$ . Then

$$\mathbb{S}_{f,g}(x, y) = xy - ((c^{1/\beta}x^{\alpha/\beta})y)^\beta = xy - cx^\alpha y^\beta,$$

so  $\mathbb{S}_{f,g} = \text{GTF}_{c,\alpha,\beta}$ , and hence  $\mathcal{S}(\mathcal{D}_{r,n,q}, U_f, W_g)$  is equivalent to  $\mathcal{S}(\text{GTF}_{c,\alpha,\beta})$ .

**Remark 2.** Recall from (2) that every (pre)semifield multiplication can be written as

$$\mathbb{S}(x, y) = \sum_{i=0}^{n-1} l_i(x)y^{q^i},$$

for some  $l_i$ . Then taking  $g_i(z) = z^{q^i}$ , and  $f_i(x) = l_i(x)^{q^{-i}}$ , we get that

$$\mathbb{S}_{f,g}(x, y) = \mathbb{S}(x, y),$$

and so  $\mathcal{S}(\mathbb{S}) \simeq \mathcal{S}(\mathcal{D}_{r,n,q}, U_f, W_g)$ .

The triple  $(\mathcal{D}_{r,n,q}, U_f, W_g)$ , with these particular  $n$ -tuples of endomorphisms  $f_i$  and  $g_i$ , is precisely the BEL-configuration which was used in [3], Theorem 4.1, to show that every (pre)semifield can be constructed from some BEL-configuration in  $V(n^2, q)$ . So for  $r = n$ , the approach using the representation of the subspaces as  $U_f$  and  $W_g$ , is the same as in the proof of [3, Theorem 4.1]. But the advantage of the viewpoint taken here is that this explicit multiplication can not only be obtained for  $r = n$ , but for any  $r \geq 2$ .

**Remark 3.** As pointed out in the proof of Theorem 3, it follows from the BEL-construction (Theorem 2) that  $\mathcal{S}(\mathcal{D}_{r,n,q}, U_f, W_g)$  forms a semifield spread, and this was proven geometrically in [3]. It then follows that  $\mathbb{S}_{f,g}$  is a (pre)semifield, with multiplication defined in (13). However, with the explicit descriptions of the subspaces  $U_f$  and  $W_g$ , defined by the  $r$ -tuples of endomorphisms  $f_i$  and  $g_i$ , we are able to prove directly that the multiplication (13) defines a presemifield.

*Proof.* It is clear that this multiplication is bilinear in  $x$  and  $y$  over  $\mathbb{F}_q$ , and hence it only remains to show that  $\mathbb{S}_{f,g}$  has no zero divisors. Suppose that  $\sum_{i=1}^r g_i(f_i(x)y) = 0$  for some  $x, y \neq 0$ . Then  $(f_1(x)y, \dots, f_r(x)y) \in W_g$ . Hence  $(f_1(x), \dots, f_r(x)) \in \tilde{\mathcal{B}}(W_g) \cap U_f$ , a contradiction on  $(\mathcal{D}_{r,n,q}, U_f, W_g)$  being a BEL-configuration by Lemma 2.  $\square$

Consequently, this implies that  $\mathcal{S}(\mathbb{S}_{f,g})$  is a semifield spread. This provides an alternative proof of the fact that the BEL-construction gives a semifield spread.

We know from [3] that every presemifield can be constructed from a BEL-configuration in  $V(n^2, q)$ , and we have seen above that the generalized twisted fields can be constructed for  $r = 2$ , and there are many other examples. For instance, whenever we have a multiplication where some  $l_i(x)$  or  $r_j(y)$ , as defined in (2), are zero, we can find a BEL-configuration for  $r < n$ , see also [3, Remark 4.2].

The following lemma gives a geometric sufficient condition to obtain a BEL-configuration for smaller  $r$ .

**Theorem 4.** Suppose  $(\mathcal{D}, U, W)$  is a BEL-configuration in  $V(rn, q)$ . If  $W$  contains an element of  $\mathcal{D}$ , then there exists a BEL-configuration  $(\mathcal{D}', U', W')$  in  $V((r-1)n, q)$  such that  $\mathcal{S}(\mathcal{D}, U, W) = \mathcal{S}(\mathcal{D}', U', W')$ .

*Proof.* Let  $\mathcal{D} = \mathcal{D}_{r,n,q}$ ,  $U = U_f$ ,  $W = W_g$ , so  $\mathcal{S}(\mathcal{D}, U, W) \simeq \mathcal{S}(\mathbb{S}_{f,g})$ . Suppose  $\mathcal{B}(v) \leq W_g$ . Then  $\sum g_i(v_i x) = 0$  for all  $x \in \mathbb{F}_{q^n}$ . Without loss of generality, we may assume that  $v_k = 1$  for some  $k \in \{1, \dots, r\}$ . Then  $g_k(x) = -\sum_{i \neq k} g_i(v_i x)$  for all  $x \in \mathbb{F}_{q^n}$ . So

$$\mathbb{S}_{f,g}(x, y) = \sum_{i \neq k} g_i((f_i(x) - v_i f_k(x))y).$$

Defining  $f'_i(x) = f_i(x) - v_i f_k(x)$ , and  $g' = (g_1, \dots, g_{k-1}, g_{k+1}, \dots, g_r)$ ,  $f' = (f'_1, \dots, f'_{k-1}, f'_{k+1}, \dots, f'_r)$ , we get that  $\mathbb{S}_{f,g} = \mathbb{S}_{f',g'}$ , and hence  $\mathcal{S}(\mathbb{S}_{f,g}) = \mathcal{S}(\mathbb{S}_{f',g'})$ . It follows that  $(\mathcal{D}_{r-1,n,q}, U_{f'}, W_{g'})$  is a BEL-configuration in  $V((r-1)n, q)$  satisfying  $\mathcal{S}(\mathcal{D}, U, W) = \mathcal{S}(\mathcal{D}_{r-1,n,q}, U_{f'}, W_{g'})$ .  $\square$

### 3 BEL-configurations and polarities

In this section we will show how to find a BEL-configuration for the dual spread of  $\mathcal{S}(\mathcal{D}, U, W)$ . As a corollary, we will get a nice description of symplectic semifields in the context of BEL-configurations.

Let  $\rho$  be any polarity on  $V(rn, q)$ , and let  $b_\rho$  denote its associated nondegenerate (symmetric bilinear, symplectic, or hermitian) form. For a spread  $\mathcal{D}$ , define the set  $\mathcal{D}_\rho$  as follows:

$$\mathcal{D}_\rho = \{H^\rho : \dim(H) = rn - n \text{ and } H \text{ is generated by elements of } \mathcal{D}\}. \quad (14)$$

**Lemma 4.** *Let  $\mathcal{D}$  be a Desarguesian spread in  $V(rn, q)$ , and  $\rho$  any nondegenerate polarity. Then  $\mathcal{D}_\rho$  is again a Desarguesian spread.*

*Proof.* We assume without loss of generality that  $\mathcal{D} = \mathcal{D}_{r,n,q}$ . Then the elements of  $\mathcal{D}$  correspond to 1-dimensional  $\mathbb{F}_{q^n}$ -subspaces of  $(\mathbb{F}_{q^n})^r$ , and so  $kn$ -dimensional subspaces generated by elements of  $\mathcal{D}$  correspond to  $k$ -dimensional  $\mathbb{F}_{q^n}$ -subspaces of  $(\mathbb{F}_{q^n})^r$ . For a formalized description of this “field reduction” see [17].

Let  $H_1^\rho, H_2^\rho$  be distinct elements of  $\mathcal{D}_\rho$ . Any intersection of subspaces spanned by elements of a Desarguesian spread is partitioned by elements of that spread. Hence  $\dim(\langle H_1, H_2 \rangle) = rn$ , and so  $\dim(H_1^\rho \cap H_2^\rho) = 0$ , proving that  $\mathcal{D}_\rho$  is a spread.

Suppose  $r = 2$ . In this case  $\mathcal{D}_\rho = \mathcal{D}^\rho = \{S^\rho : S \in \mathcal{D}\}$ , and the proof easily follows from the fact that the dual of a semifield spread of  $V(2n, q)$  corresponds to the transpose of the semifield, and the Desarguesian spread corresponds to the field.

Suppose  $r > 2$ . Then  $\mathcal{D}_\rho$  is Desarguesian if and only if every subspace spanned by elements of  $\mathcal{D}_\rho$  is partitioned by elements of  $\mathcal{D}_\rho$ . Let  $S = \langle H_1^\rho, \dots, H_k^\rho \rangle$ , with  $\dim(S) = nk$ . Then  $S^\rho = \bigcap_{i=1..k} H_i$ , and  $\dim(S^\rho) = n(r - k)$ . Now there are precisely  $\frac{q^{nk}-1}{q^n-1}$  subspaces  $H_i$  such that  $S^\rho \leq H_i$  and  $H_i$  is an  $(rn - n)$ -dimensional subspace spanned by elements of  $\mathcal{D}$ . But then  $H_i^\rho \leq S$  for all  $i$ , and so the set  $\{H_i^\rho : i \in 1, \dots, \frac{q^{nk}-1}{q^n-1}\} \subset \mathcal{D}_\rho$  partitions  $S$ , proving that  $\mathcal{D}_\rho$  is Desarguesian.  $\square$

**Theorem 5.** *Suppose  $\rho$  is a nondegenerate polarity in  $V(rn, q)$ , and  $\mathcal{D} = \mathcal{D}_{r,n,q}$ . Then  $(\mathcal{D}, U, W)$  is a BEL-configuration if and only if  $(\mathcal{D}_\rho, W^\rho, U^\rho)$  is a BEL-configuration.*

*Proof.* Suppose  $(\mathcal{D}_\rho, W^\rho, U^\rho)$  is not a BEL-configuration. Then there exists some  $H^\rho \in \mathcal{D}_\rho$  such that  $H^\rho \cap U^\rho$  and  $H^\rho \cap W^\rho$  are both non-trivial. Now

$$H \cap U = H^{\rho\rho} \cap U^{\rho\rho} = \langle H^\rho, U^\rho \rangle^\rho,$$

and so  $\dim(H \cap U) = \dim(\langle H^\rho, U^\rho \rangle^\rho) > 0$ . By the definition of  $\mathcal{D}_\rho$ ,  $H$  is spanned by elements of  $\mathcal{D}$ , and hence there exists an element  $T \in \mathcal{D}$  such that  $T \subset H$  and  $T \in \mathcal{B}_\mathcal{D}(U)$ . On the other hand, since  $H^\rho \in \mathcal{B}_{\mathcal{D}_\rho}(W^\rho)$ , we have  $\dim(H \cap W) > rn - 2n$ . This implies that each element of  $\mathcal{D}$  which is contained in  $H$ , must intersect  $W$  non-trivially, i.e. must belong to  $\mathcal{B}_\mathcal{D}(W)$ . This implies that also  $T \in \mathcal{B}_\mathcal{D}(W)$ , a contradiction, as  $(\mathcal{D}, U, W)$  is a BEL-configuration. It follows that  $(\mathcal{D}_\rho, W^\rho, U^\rho)$  is a BEL-configuration. For the converse it suffices to note that  $(\mathcal{D}_\rho)_\rho = \mathcal{D}$ .  $\square$

Hence, by Theorem 5, from a semifield spread  $\mathcal{S}(\mathcal{D}, U, W)$  and a polarity  $\rho$  we obtain a semifield spread  $\mathcal{S}(\mathcal{D}_\rho, W^\rho, U^\rho)$ . However, as we will show, this operation does not induce an extension of the Knuth orbit. First we will show that different choices of the polarity  $\rho$  give equivalent semifield spreads. Subsequently, we will show that this operation corresponds to the dual operation on spreads, or in other words the transpose operation on semifields.

Define a nondegenerate symmetric bilinear form  $b$  on  $V(rn, q)$  by

$$b(u, v) = b((u_1, \dots, u_r), (v_1, \dots, v_r)) := \text{tr} \left( \sum_{i=1}^r u_i v_i \right), \quad (15)$$

where  $\text{tr}$  denotes the field trace from  $\mathbb{F}_{q^n}$  to  $\mathbb{F}_q$ . Denote the corresponding polarity by  $\perp$ , i.e. if  $M$  is any subspace of  $V(rn, q)$ , then

$$M^\perp = \{v : v \in V(rn, q) \mid b(u, v) = 0 \ \forall u \in M\}. \quad (16)$$

**Lemma 5.** *If  $\mathcal{D} = \mathcal{D}_{r,n,q}$  and  $\perp$  denotes the polarity as in (16), then  $\mathcal{D}_\perp = \mathcal{D}$ .*

*Proof.* If  $H$  is a subspace of dimension  $rn - n$  spanned by elements of  $\mathcal{D}$ , then  $H^\perp \in \mathcal{D}$ , and so  $\mathcal{D}_\perp = \mathcal{D}$ .  $\square$

**Theorem 6.** *Let  $\mathcal{D} = \mathcal{D}_{r,n,q}$ . If  $\rho$  is a nondegenerate polarity of  $V(rn, q)$ , then the BEL-configurations  $(\mathcal{D}_\rho, W^\rho, U^\rho)$  and  $(\mathcal{D}, W^\perp, U^\perp)$  are equivalent.*

*Proof.* First we claim that there exists some  $\phi \in \Gamma\text{L}(rn, q)$  such that

$$b_\rho(u, v) = b(u, v^\phi)$$

for all  $u, v \in V(rn, q)$ , where  $b$  is as defined in (15) and  $b_\rho$  is the form associated to the polarity  $\rho$ . If we take the elements of  $V(rn, q)$  to be column vectors of length  $rn$  over  $\mathbb{F}_q$ , then for every symmetric bilinear, symplectic or hermitian form  $b_\rho$  on  $V(rn, q)$  there exists an invertible  $rn \times rn$  matrix  $B_\rho$  with entries in  $\mathbb{F}_q$  and an  $\mathbb{F}_q$ -automorphism  $\sigma$  such that  $b_\rho(u, v) = u^T B_\rho v^\sigma$ . Hence defining  $\phi \in \Gamma\text{L}(rn, q)$  by  $v^\phi = B_\perp^{-1} B_\rho v^\sigma$ , where  $B_\perp$  is the matrix corresponding to  $b$  as defined in (15), the claim is proven.

Hence for any subspace  $M$ , we have that  $v \in M^\rho$  if and only if  $b(u, v^\phi) = 0$  for all  $u \in M$ , if and only if  $v^\phi \in M^\perp$ , implying  $M^\rho = M^{\perp \phi^{-1}}$ . It also follows

that  $\mathcal{D}_\rho = (\mathcal{D}_\perp)^{\phi^{-1}}$ . Moreover, by Lemma 5,  $\mathcal{D}_\perp = \mathcal{D}$ . Then  $(\mathcal{D}_\rho, W^\rho, U^\rho) = ((\mathcal{D}_\perp)^{\phi^{-1}}, W^{\perp\phi^{-1}}, U^{\perp\phi^{-1}}) = (\mathcal{D}^{\phi^{-1}}, W^{\perp\phi^{-1}}, U^{\perp\phi^{-1}})$ . Hence by Remark 1, we can apply  $\phi$  to get that  $\mathcal{S}(\mathcal{D}_\rho, W^\rho, U^\rho)$  is equivalent to  $\mathcal{S}(\mathcal{D}, W^\perp, U^\perp)$ , as claimed.  $\square$

**Lemma 6.** *Consider the subspace  $U_f$  of  $V(rn, q)$  as in Lemma 3 for some  $r$ -tuple  $f = (f_1, f_2, \dots, f_r)$  of  $\mathbb{F}_q$ -endomorphisms of  $\mathbb{F}_{q^n}$ . Then  $U_f^\perp = W_{\hat{f}}$ , where  $\hat{f} := (\hat{f}_1, \dots, \hat{f}_r)$ , and*

$$W_{\hat{f}} := \{(x_1, x_2, \dots, x_r) : x_i \in \mathbb{F}_{q^n} \mid \sum_i \hat{f}_i(x_i) = 0\}.$$

*Proof.* Now  $v \in U_f^\perp$  if and only if

$$\begin{aligned} b((f_1(u), \dots, f_r(u)), v) &= \text{tr}\left(\sum_i f_i(u)v_i\right) \\ &= \text{tr}\left(u \sum_i \hat{f}_i(v_i)\right) = 0 \end{aligned}$$

for all  $u \in \mathbb{F}_{q^n}$ . But this occurs if and only if  $\sum_i \hat{f}_i(v_i) = 0$ , i.e. if and only if  $v \in W_{\hat{f}}$ , proving the claim.  $\square$

**Lemma 7.** *Suppose  $f$  and  $g$  are  $r$ -tuples of endomorphisms such that  $\mathbb{S}_{f,g}$  is a semifield, with multiplication as defined in (13). Then  $\mathbb{S}_{f,g}^t = \mathbb{S}_{\hat{g}, \hat{f}}$ .*

*Proof.* If  $R_y$  denotes the endomorphism of right multiplication by  $y$  in  $\mathbb{S}_{f,g}$ , then

$$R_y = \sum_i g_i y f_i.$$

Hence  $\hat{R}_y = \sum_i \hat{f}_i \hat{g}_i y$ . But  $\hat{y} = y$ , and so

$$\begin{aligned} \mathbb{S}_{f,g}^t(x, y) &= \sum_i (\hat{f}_i y \hat{g}_i)(x) \\ &= \sum_i \hat{f}_i(\hat{g}_i(x)y) \\ &= \mathbb{S}_{\hat{g}, \hat{f}}(x, y), \end{aligned}$$

as claimed.  $\square$

**Theorem 7.** *Let  $\mathcal{D} = \mathcal{D}_{r,n,q}$ ,  $\rho$  a nondegenerate polarity and  $(\mathcal{D}, U, W)$  a BEL-configuration in  $V(rn, q)$ . Then the semifield spreads  $\mathcal{S}(\mathcal{D}_\rho, W^\rho, U^\rho)$  and  $\mathcal{S}(\mathcal{D}, U, W)$  are dual to each other.*

*Proof.* Let  $(U, W) = (U_f, W_g)$  for some  $f, g$ . By Theorem 3,  $\mathcal{S}(\mathcal{D}, U, W)$  is equivalent to  $\mathcal{S}(\mathbb{S}_{f,g})$ . By Lemma 6,  $\mathcal{S}(\mathcal{D}, W^\perp, U^\perp) = \mathcal{S}(\mathcal{D}, U_{\hat{g}}, W_{\hat{f}})$ , which is equivalent to  $\mathcal{S}(\mathbb{S}_{\hat{g}, \hat{f}})$ . By Lemma 7,  $\mathbb{S}_{f,g}^t = \mathbb{S}_{\hat{g}, \hat{f}}$ , and hence  $\mathcal{S}(\mathbb{S}_{f,g}^t) = \mathcal{S}(\mathbb{S}_{\hat{g}, \hat{f}})$ , proving that  $\mathcal{S}(\mathcal{D}, W^\perp, U^\perp)$  is equivalent to  $\mathcal{S}(\mathbb{S}_{f,g}^t)$ . It follows that  $\mathcal{S}(\mathcal{D}, W^\perp, U^\perp)$  and  $\mathcal{S}(\mathcal{D}, U, W)$  are dual to each other. Theorem 6 completes the proof.  $\square$

**Remark 4.** We may define now an operation on the equivalence classes  $[U, W]$  defined in Remark 1, where the Desarguesian spread is taken to be  $\mathcal{D}_{r,n,q}$ . Define

$$[U, W]^t = [W^\perp, U^\perp]. \quad (17)$$

Then this operation is well defined, as  $U^{\perp\phi} = U^{\phi\perp}$  for all  $\phi \in \Gamma\mathbb{L}(r, q^n)$ .

We are now ready to prove a new characterization of symplectic semifield spreads, using BEL-configurations.

**Theorem 8.** Suppose  $(\mathcal{D}_{r,n,q}, U, U^\perp)$  is a BEL-configuration in  $V(rn, q)$ , where  $\perp$  is as defined in (16). Then  $\mathcal{S}(\mathcal{D}_{r,n,q}, U, U^\perp)$  is a symplectic semifield spread. Conversely, for every symplectic semifield spread  $\mathcal{S}'$ , there exists some  $r$  and some  $U$  a subspace of dimension  $n$  in  $V(rn, q)$  such that  $\mathcal{S}'$  is equivalent to  $\mathcal{S}(\mathcal{D}_{r,n,q}, U, U^\perp)$ .

*Proof.* The first statement follows immediately from Theorem 7. For the converse, suppose  $\mathcal{S}'$  is a symplectic semifield spread. Then  $\mathcal{S}'$  is equivalent to  $\mathcal{S}(\mathbb{S})$ , where  $\mathbb{S}^{dtd}$  is some commutative presemifield. Suppose  $\mathbb{S}^{dtd}(x, y) = \sum_{i,j} c_{ij} x^{q^i} y^{q^j}$ , and let  $C$  be the  $n \times n$  matrix over  $\mathbb{F}_{q^n}$  with  $(i, j)$ -th entry  $c_{ij}$ . Since  $\mathbb{S}^{dtd}$  is commutative,  $C$  is a symmetric matrix. Hence there exist some column vectors  $v_k \in (\mathbb{F}_{q^n})^n$ ,  $k = 1, \dots, r$ , such that

$$C = \sum_{k=1}^r v_k v_k^T.$$

In other words, we write the symmetric matrix  $C$  as a sum of  $r$  symmetric matrices of rank one. If we denote the  $i$ -th coordinate of  $v_k$  by  $f_{ki}$ , then we have that  $c_{ij} = \sum_k f_{ki} f_{kj}$ , and so

$$\mathbb{S}^{dtd}(x, y) = \sum_{k=1}^r \sum_{i,j=0}^{n-1} f_{ki} f_{kj} x^{q^i} y^{q^j} = \sum_{k=1}^r \left( \sum_{i=0}^{n-1} f_{ki} x^{q^i} \right) \left( \sum_{j=0}^{n-1} f_{kj} y^{q^j} \right).$$

Now if we define endomorphisms  $f_k$  by  $f_k(x) = \sum_{i=0}^{n-1} f_{ki} x^{q^i}$ , it is clear that

$$\mathbb{S}^{dtd}(x, y) = \sum_{k=1}^r f_k(x) f_k(y).$$

Hence

$$\begin{aligned}\mathbb{S}(x, y) &= \sum_{k=1}^r \hat{f}_k(f_k(x)y) \\ &= \mathbb{S}_{f, \hat{f}}(x, y),\end{aligned}$$

and so, by Theorem 3 and Lemma 6,  $\mathcal{S}(\mathbb{S}) = \mathcal{S}(\mathbb{S}_{f, \hat{f}})$  is equivalent to  $\mathcal{S}(\mathcal{D}, U_f, U_f^\perp)$ , completing the proof.  $\square$

**Remark 5.** *Note that we do not assume in Theorem 8 that  $r \leq n$ , in contrast to Theorem 4.1 of [3]. This is because the proof relies on writing a symmetric  $n \times n$  matrix as the sum of  $r$  symmetric  $n \times n$  matrices of rank one of a specific type, that is of the form  $vv^T$  for some column vector  $v$ . This decomposition is not necessarily possible if we impose the condition  $r \leq n$ .*

## 4 Isotopy and BEL-configurations

Now we will consider further operations on BEL-configurations which preserve the BEL property. This section will follow [12], where the case  $r = n$  was considered. Afterwards, we will show how, when  $r < n$ , we can use this operation to produce non-isotopic semifields from a single BEL-configuration.

It is clear from the BEL property (Lemma 2), that if  $\phi, \phi'$  are elements of  $\Gamma\text{L}(rn, q)$  which fix the set  $\tilde{\mathcal{B}}_{\mathcal{D}}(W)$ , then  $(\mathcal{D}, U, W)$  is a BEL-configuration if and only if  $(\mathcal{D}, U^\phi, W^{\phi'})$  is a BEL-configuration. We now consider the question of when the two semifields arising from these configurations are isotopic, or in other words when the two semifield spreads are equivalent.

For the remainder of this section, we will set  $\mathcal{D} = \mathcal{D}_{r, n, q}$ .

Suppose  $W_g$  is a subspace of  $V(rn, q)$  of dimension  $rn - n$  as defined in (11). Define a map  $\psi_g$  from  $V(rn, q)$  into  $\text{End}_{\mathbb{F}_q}(\mathbb{F}_{q^n})$  by

$$\psi_g : (v_1, \dots, v_r) \mapsto \sum g_i v_i,$$

where  $\sum g_i v_i$  means the endomorphism  $z \mapsto \sum g_i(v_i z)$ .

**Lemma 8.** *The map  $\psi_g$  is injective if and only if  $W_g$  does not contain an element of  $\mathcal{D}$ .*

*Proof.* The map  $\psi_g$  is not injective if and only if there exists some  $v \neq 0$  such that  $\psi_g(v)$  is the zero map. This occurs if and only if  $\sum_i g_i(v_i x) = 0$  for all  $x \in \mathbb{F}_{q^n}$ , if and only if  $\mathcal{B}(v) = \{(v_1 x, \dots, v_r x) : x \in \mathbb{F}_{q^n}\} \leq W_g$ , proving the claim.  $\square$

Note that this condition is the same condition from Lemma 4.



**Lemma 9.** *Let  $v \in V(rn, q)^\times$ . Then  $\psi_g(v)$  is a singular endomorphism if and only if  $v \in \tilde{\mathcal{B}}(W_g)$ .*

*Proof.* We have that  $\psi_g(v)$  is singular, if and only if there exists some  $\alpha \in \mathbb{F}_{q^n}^\times$  such that  $\psi_g(v)(\alpha) = 0$ , if and only if there exists some  $\alpha \in \mathbb{F}_{q^n}^\times$  such that  $(\alpha v_1, \dots, \alpha v_r) \in W_g$ , if and only if  $v \in \tilde{\mathcal{B}}(W_g)$ , proving the claim.  $\square$

**Lemma 10.** *Suppose  $(\mathcal{D}, U_f, W_g)$  is a BEL-configuration. Then  $\psi_g(U_f)$  is a subspace of  $\text{End}_{\mathbb{F}_q}(\mathbb{F}_{q^n})$  of dimension  $n$ , in which all of its nonzero elements are nonsingular. Furthermore,  $\psi_g(U_f)$  is precisely the semifield spread set  $R(\mathbb{S}_{f,g}^d)$ .*

*Proof.* This first part follows immediately from the previous lemma. Now

$$\begin{aligned} \psi_g(U_f) &= \{y \mapsto \sum g_i(f_i(x)y) : x \in \mathbb{F}_{q^n}\} \\ &= \{y \mapsto \mathbb{S}_{f,g}(x, y) : x \in \mathbb{F}_{q^n}\} \\ &= \{L_x : x \in \mathbb{F}_{q^n}\} \\ &= R(\mathbb{S}_{f,g}^d), \end{aligned}$$

proving the claim.  $\square$

**Theorem 9.** *Suppose  $W$  is a subspace of  $V(n^2, q)$  of dimension  $n^2 - n$  such that  $W$  does not contain an element of  $\mathcal{D}$ . Suppose  $(\mathcal{D}, U, W)$  and  $(\mathcal{D}, U', W)$  are two BEL-configurations. Then  $\mathcal{S}(\mathcal{D}, U', W)$  is equivalent to  $\mathcal{S}(\mathcal{D}, U, W)$  or the dual of  $\mathcal{S}(\mathcal{D}, U, W)$  if and only if there exists some  $\phi \in \text{Stab}(\tilde{\mathcal{B}}(W)) \leq \Gamma\text{L}(n^2, q)$  such that  $U' = U^\phi$ .*

*Proof.* By Lemma 3, we may write  $U = U_f$ ,  $U' = U_h$ , and  $W = W_g$ . By Lemma 10, we can identify  $V(n^2, q)$  with  $\text{End}_{\mathbb{F}_q}(\mathbb{F}_{q^n})$  via the map  $\psi_g$ , which is injective by Lemma 8. Furthermore, the set of singular endomorphisms is precisely the set  $\psi_g(\tilde{\mathcal{B}}(W_g))$ . Then  $\psi_g(U_f)$  and  $\psi_g(U_h)$  are subspaces corresponding to the semifield spread sets defined by  $\mathbb{S}_{f,g}^d$  and  $\mathbb{S}_{h,g}^d$ .

A map  $\phi$  is in  $\text{Stab}(\tilde{\mathcal{B}}(W_g))$  if and only if  $\psi_g \phi \psi_g^{-1}$  fixes the set of singular endomorphism in  $\text{End}_{\mathbb{F}_q}(\mathbb{F}_{q^n})$ .

Now the invertible semilinear maps preserving the set of singular endomorphisms are precisely those of the form

$$A \mapsto X A^\sigma Y$$

or

$$A \mapsto X \hat{A}^\sigma Y$$

for some nonsingular endomorphisms  $X, Y$ , and some  $\sigma \in \text{Aut}(\mathbb{F}_q)$ .

Then

$$\begin{aligned}
& \mathcal{S}(\mathcal{D}, U_h, W_g) \simeq \mathcal{S}(\mathcal{D}, U_f, W_g) \text{ or the dual of } \mathcal{S}(\mathcal{D}, U_f, W_g) \\
& \quad \Leftrightarrow \\
& \quad \mathcal{S}(\mathbb{S}_{h,g}) \simeq \mathcal{S}(\mathbb{S}_{f,g}) \text{ or } \mathcal{S}(\mathbb{S}_{f,g}^t) \\
& \quad \Leftrightarrow \\
& \quad \mathbb{S}_{h,g} \text{ is isotopic to } \mathbb{S}_{f,g} \text{ or } \mathbb{S}_{f,g}^t \\
& \quad \Leftrightarrow \\
& \quad \mathbb{S}_{h,g}^d \text{ is isotopic to } \mathbb{S}_{f,g}^d \text{ or } \mathbb{S}_{f,g}^{td} \\
& \quad \Leftrightarrow \\
& \text{there exist invertible endomorphisms } X, Y \text{ and some } \sigma \in \text{Aut}(\mathbb{F}_q) \text{ such that} \\
& \quad \psi_g(U_f) = X\psi_g(U_h)^\sigma Y \text{ or } \psi_g(U_f) = X\widehat{\psi_g(U_h)}^\sigma Y \\
& \quad \Leftrightarrow \\
& \text{there exists some } \rho \in \text{GL}(\text{End}_{\mathbb{F}_q}(\mathbb{F}_{q^n}), q) \text{ fixing the set of singular} \\
& \quad \text{endomorphisms such that } \psi_g(U_f) = \rho\psi_g(U_h) \\
& \quad \Leftrightarrow \\
& \text{there is a map } \phi = \psi_g^{-1}\rho^{-1}\psi_g \in \text{GL}(n^2, q) \text{ fixing } \tilde{\mathcal{B}}(W) \text{ such that } U_h = U_f^\phi.
\end{aligned}$$

□

**Remark 6.** *This theorem and its proof closely follow [13], Theorem 17. That theorem is stated for a specific  $W = W_g$ , where  $g = (1, \sigma, \dots, \sigma^{n-1})$  and  $\sigma(x) = x^q$  for all  $x \in \mathbb{F}_{q^n}$ . The extension to arbitrary  $W$  is trivial. However there is a small error in that theorem, which we rectify here.*

*The inaccuracy occurs on page 909: in the line “In particular,  $\varphi$  fixes both families of maximal subspaces of the Segre variety, and hence, by Corollary 12,  $\phi$  fixes  $\mathcal{B}(W)$ .”, the  $\mathcal{B}(W)$  should instead read  $\tilde{\mathcal{B}}(W)$ .*

*For the converse then, again  $\mathcal{B}(W)$  should be replaced by  $\tilde{\mathcal{B}}(W)$ , and hence rather than implying an isotopy between the two semifields under consideration, it implies that the first is either isotopic to the second, or isotopic to the transpose of the second.*

*The above proof is self contained, and does not rely on Theorem 17 of [13], though the method is the same.*

## 5 BEL-configurations in $V(2n, q)$

### 5.1 Action of the stabilizer of $\tilde{\mathcal{B}}(W)$

We showed in the previous section that if  $(\mathcal{D}, U, W)$  is a BEL-configuration in  $V(n^2, q)$ , and  $W$  does not contain an element of  $\mathcal{D}$ , then the elements of the set  $\{\mathcal{S}(\mathcal{D}, U^\phi, W) : \phi \in \text{Stab}\tilde{\mathcal{B}}(W)\}$  are all equivalent to  $\mathcal{S}(\mathcal{D}, U, W)$  or  $\mathcal{S}(\mathcal{D}, U, W)^\epsilon$ , and so we do not get an extension of the Knuth orbit in this case.

However, when  $r < n$ , the situation is different. Firstly, it is not clear whether if  $\mathcal{S}(\mathcal{D}, U, W)$  and  $\mathcal{S}(\mathcal{D}, U', W)$  are equivalent then there must exist a  $\phi$  fixing  $\tilde{\mathcal{B}}(W)$  such that  $U' = U^\phi$ . Conversely, we will now present an example

in  $V(2n, q)$  where  $\mathcal{S}(\mathcal{D}, U^\phi, W)$  is not equivalent to any Knuth derivative of  $\mathcal{S}(\mathcal{D}, U, W)$ . The example will concern generalized twisted fields.

Let  $r = 2$ , and let  $g = (1, -\beta)$ , where  $\beta \in \text{Aut}(\mathbb{F}_{q^n})$ , and  $\beta$  has fixed field  $\mathbb{F}_{q^{n/t}}$ . Put

$$W := W_g = \{(x^\beta, x) : x \in \mathbb{F}_{q^n}\}. \quad (18)$$

In [16], this subspace and the set  $\tilde{\mathcal{B}}(W)$  was investigated, and the following properties proved. Recall that we are assuming the Desarguesian spread  $\mathcal{D} = \mathcal{D}_{2,n,q}$ .

In what follows  $N$  denotes the norm function from  $\mathbb{F}_{q^n}$  to  $\mathbb{F}_{q^{n/t}}$ , i.e.  $N(a) = aa^\beta \dots a^{\beta^{t-1}}$ .

**Theorem 10.** (i)  $\tilde{\mathcal{B}}(W)$  is a nonsingular hypersurface of degree  $n$ , defined by

$$\tilde{\mathcal{B}}(W) = \{(a, b) : a, b \in \mathbb{F}_{q^n} \mid N(a) = N(b) \neq 0\}.$$

(ii) The subspaces of dimension  $n$  contained in  $\tilde{\mathcal{B}}(W)$  are precisely those of the form  $S_{\gamma,k} := \{(x, kx^\gamma) : x \in \mathbb{F}_{q^n}\}$ , where  $k \in \mathbb{F}_{q^n}$ ,  $N(k) = 1$  and  $\gamma \in \text{Aut}(\mathbb{F}_{q^n} : \mathbb{F}_{q^{n/t}})$ . These can be divided into  $t$  systems which each partition  $\tilde{\mathcal{B}}(W)$ , by defining  $\mathcal{S}_\gamma := \{S_{\gamma,k} : k \in \mathbb{F}_{q^n} \mid N(k) = 1\}$  for each  $\gamma \in \text{Aut}(\mathbb{F}_{q^n} : \mathbb{F}_{q^{n/t}})$ .

(iii) Let  $G$  denote the setwise stabilizer of  $\tilde{\mathcal{B}}(W)$  in  $\text{GL}(2n, q)$ . Then  $G$  contains the elements

$$\begin{aligned} \phi_{k,m,\gamma,\delta} : (a, b) &\mapsto (ka^\gamma, mb^\delta); \\ \phi'_{k,m,\gamma,\delta} : (a, b) &\mapsto (kb^\gamma, ma^\delta) \end{aligned}$$

for  $\gamma, \delta \in \text{Aut}(\mathbb{F}_{q^n} : \mathbb{F}_{q^{n/t}})$ ,  $k, m \in \mathbb{F}_{q^n}$  such that  $N(k) = N(m) \neq 0$ . These form a subgroup of  $G$ . If  $n$  is prime, then  $G$  contains no other elements.

So we can consider BEL-configurations of the form  $(\mathcal{D}, U, W)$  in  $V(2n, q)$ , and investigate the action of  $G$ . If  $U = U_f$ , then  $\mathcal{S}(\mathcal{D}, U_f, W)$  is equivalent to  $\mathcal{S}(\mathbb{S}_{f,g})$ , and

$$\mathbb{S}_{f,g}(x, y) = f_1(x)y - (f_2(x)y)^\beta.$$

Let  $\phi = \phi_{1,1,1,\gamma}$ , that is  $\phi((a, b)) = (a, b^\gamma)$ , where  $\gamma \in \text{Aut}(\mathbb{F}_{q^n} : \mathbb{F}_q)$ . By the above,  $\phi \in G$ . Then  $U_f^\phi = U_h$ , with  $h = (f_1, \gamma \circ f_2)$ . Hence  $\mathcal{S}(\mathcal{D}, U_f^\phi, W) = \mathcal{S}(\mathcal{D}, U_h, W)$ , which is equivalent to  $\mathcal{S}(\mathbb{S}_{h,g})$ , and

$$\mathbb{S}_{h,g}(x, y) = f_1(x)y - (f_2(x)^\gamma y)^\beta.$$

Now let  $f = (1, c^{1/\beta}\alpha/\beta)$ , so  $U_f = \{(x, c^{1/\beta}x^{\alpha/\beta}) : x \in \mathbb{F}_{q^n}\}$ . Then

$$\mathbb{S}_{f,g}(x, y) = xy - cx^\alpha y^\beta,$$

and so  $\mathbb{S}_{f,g}(x, y) = \text{GTF}_{c,\alpha,\beta}$ . Then

$$\mathbb{S}_{h,g} = xy - c^\gamma x^{\gamma\alpha} y^\beta,$$

and so  $\mathbb{S}_{h,g} = \text{GTF}_{c^\gamma, \alpha^\gamma, \beta}$ .

It is clear from Theorem 1 that in general these are nonisotopic (pre)semifields. In fact, if  $\gamma\alpha = \beta$ , then we get a presemifield isotopic to a finite field.

So this action can indeed produce nonisotopic semifields, or equivalently nonequivalent semifield spreads.

Note that we may also allow  $G$  to act on  $W_g$ , and still retain the BEL property. If we take  $\phi = \phi_{k,m,\gamma,\delta}$ ,  $\phi' = \phi_{k',m',\gamma',\delta'}$ , then after some calculations we see that

$$\mathcal{S}(\mathcal{D}, U_f, W_g) \simeq \mathcal{S}(\text{GTF}(c, \alpha, \beta)) \quad (19)$$

$$\mathcal{S}(\mathcal{D}, U_f^\phi, W_g^{\phi'}) \simeq \mathcal{S}(\text{GTF}(c', \alpha', \beta')) \quad (20)$$

where  $\alpha' = \frac{\alpha\gamma'\delta}{\delta'\gamma}$ ,  $\beta' = \frac{\beta\gamma'}{\delta'}$ , and

$$c' = \frac{k'}{m'} \frac{m^{\beta'}}{k^{\alpha'}} c^{\beta'\delta/\beta}.$$

Hence from the single BEL-configuration  $(\mathcal{D}, U_f, W_g)$  corresponding to the generalized twisted field  $\text{GTF}_{c,\alpha,\beta}$ , we can produce all generalized twisted fields  $\text{GTF}_{c',\alpha',\beta'}$  such that  $N(c) = N(c')$ , as well as the finite field.

## 5.2 A group of order 8 acting on equivalence classes $[U, W]$

In [3], it was noted that if  $(\mathcal{D}, U, W)$  is a BEL-configuration in  $V(2n, q)$ , then  $\dim(U) = \dim(W) = n$ , and condition 2 of Lemma 2 becomes symmetric in  $U$  and  $W$ . Hence we have the following.

**Lemma 11.** *In  $V(2n, q)$ ,  $(\mathcal{D}, U, W)$  is a BEL-configuration if and only if  $(\mathcal{D}, W, U)$  is a BEL-configuration.*

This operation is known as switching. We denote  $\mathcal{S}(\mathcal{D}, W, U) = \mathcal{S}(\mathcal{D}, U, W)^s$ . Taking  $\mathcal{D} = \mathcal{D}_{r,n,q}$ , we similarly define an action on the equivalence classes defined in Remark 1 by  $[U, W]^s := [W, U]$ . Note that it remains to be shown that this is well defined on equivalence classes of semifield spreads.

Together with the transpose operation defined in (17), this gives a group of order 4 acting on equivalence classes  $[U, W]$ . In this section, we will define a new operation  $e$ , which will extend this to a group of order 8.

First, we show how we can compute a multiplication corresponding to  $\mathcal{S}(\mathcal{D}, W, U)$ . This was calculated in [3] only for the class of semifields which are two dimensional over a nucleus. We will again assume  $\mathcal{D} = \mathcal{D}_{r,n,q}$  for the remainder of this section.

**Theorem 11.** Let  $\mathcal{D} = \mathcal{D}_{r,n,q}$ . Suppose  $(\mathcal{D}, U, W)$  is a BEL-configuration in  $V(2n, q)$ . Then there exist  $a, b \in \text{End}_{\mathbb{F}_q}(\mathbb{F}_{q^n})$  such that  $\mathcal{S}(\mathcal{D}, U, W)$  is equivalent to  $\mathcal{S}(\mathbb{S})$ , where

$$\mathbb{S}(x, y) = xy + b(a(x)y),$$

and  $\mathcal{S}(\mathcal{D}, U, W)^s$  is equivalent to  $\mathcal{S}(\mathbb{S}')$ , where

$$\mathbb{S}'(x, y) = xy + a(b(x)y).$$

*Proof.* Recall that  $\mathcal{S}(\mathcal{D}, U, W) \simeq \mathcal{S}(\mathcal{D}, U^\phi, W^\phi)$  for any  $\phi \in \text{GL}(2, q^n)$ . Hence without loss of generality, we may assume that  $U$  intersects  $S_\infty = \{(0, x) : x \in \mathbb{F}_{q^n}\}$  trivially, and  $W$  intersects  $S_0 = \{(x, 0) : x \in \mathbb{F}_{q^n}\}$  trivially. Thus we may assume  $U = U_{(1,a)}$ , and  $W = W_{(1,b)}$  for some endomorphisms  $a, b$ . Hence by Theorem 3,  $\mathcal{S}(\mathcal{D}, U, W)$  is equivalent to  $\mathcal{S}(\mathbb{S}_{(1,a),(1,b)}) = \mathcal{S}(\mathbb{S})$ .

Now it is straightforward to check that  $U = W_{(a,-1)}$  and  $W = U_{(-b,1)}$ . Hence by Theorem 3,  $\mathcal{S}(\mathcal{D}, U, W)^s = \mathcal{S}(\mathcal{D}, W, U)$  is equivalent to  $\mathcal{S}(\mathbb{S}_{(-b,1),(a,-1)}) = \mathcal{S}(\mathbb{S}')$ , completing the proof.  $\square$

Hence in order to classify semifields which can be constructed from a BEL-configuration with  $r = 2$ , it suffices to consider pairs of endomorphisms  $(a, b)$  such that

$$\frac{b(a(x)y)}{xy} \neq -1 \quad \forall x, y \in \mathbb{F}_{q^n}^\times.$$

Note that if  $q > 2$ , we may also assume that  $U$  intersects  $S_0$  trivially and  $W$  intersects  $S_\infty$  trivially, and hence that  $a$  and  $b$  are invertible. A simple counting argument shows that if  $q > 2$ , there exist two elements of  $\mathcal{D}$  not contained in  $B(U) \cup B(W)$ , and as  $\text{GL}(2, q^n)$  acts 2-transitively on  $\mathcal{D}$ , the assertion holds.

Now we will define a new operation on pairs of subspaces of dimension  $n$  in  $V(2n, q)$  which preserves the BEL property. Consider condition 5 of Lemma 2, which says that no nonzero vectors  $u \in U$  and  $w \in W$  are  $\mathbb{F}_{q^n}$ -multiples of each other. This implies that

$$\det \begin{bmatrix} u_1 & u_2 \\ w_1 & w_2 \end{bmatrix} \neq 0$$

for all  $0 \neq u = (u_1, u_2) \in U$ ,  $0 \neq w = (w_1, w_2) \in W$ .

As before, we may take  $U = U_{(1,a)}$ ,  $W = U_{(b,-1)}$ . Then

$$\det \begin{bmatrix} u_1 & u_2 \\ w_1 & w_2 \end{bmatrix} = \det \begin{bmatrix} x & a(x) \\ b(y) & -y \end{bmatrix} = -(xy + a(x)b(y)) \neq 0$$

for all  $x, y \in \mathbb{F}_{q^n}^\times$ . Hence this above formula defines a (pre)semifield multiplication.

Removing the minus sign, and taking the transpose-dual of this, we get that

$$\mathbb{S}'(x, y) = xy + \hat{a}(b(x)y)$$

defines a (pre)semifield multiplication.

Recall the symplectic polarity  $\epsilon$  defined on  $V(2n, q)$  in (6). Then it can be seen that  $U^\epsilon = U_{(1, \hat{a})} = W_{(\hat{a}, -1)}$ , and so  $\mathcal{S}(\mathcal{S}') \simeq \mathcal{S}(\mathcal{D}, W, U^\epsilon)$ , and  $\mathcal{S}(\mathcal{D}, W, U^\epsilon)$  is a BEL-configuration. Hence, switching  $W$  and  $U^\epsilon$ , we get that  $(\mathcal{D}, U^\epsilon, W)$  is a BEL-configuration, and we have proved the following.

**Theorem 12.** *Suppose  $(\mathcal{D}, U, W)$  is a BEL-configuration in  $V(2n, q)$ . Then  $(\mathcal{D}, U^\epsilon, W)$  is also a BEL-configuration.*

As  $M^{\phi\epsilon} = M^{\epsilon\phi}$  for all  $\phi \in \Gamma(2, q^n)$ , we can define an operation  $e$  on the equivalence classes defined in Remark 1 by  $[U, W] \mapsto [U^\epsilon, W]$ .

Hence we have shown that the following three actions preserve the BEL property.

$$\begin{aligned} t : [U, W] &\mapsto [W^\perp, U^\perp] \\ s : [U, W] &\mapsto [W, U] \\ e : [U, W] &\mapsto [U^\epsilon, W]. \end{aligned}$$

Each of these operations are involutions, and together they define a group of order 8, as they satisfy  $ese = t$ ,  $st = ts$ . Hence from a single BEL-configuration in  $V(2n, q)$ , we can produce up to 4 Knuth orbits, and hence up to 24 isotopy classes.

We now present a table containing a multiplication representing each of these isotopy classes. We will let  $U = U_{(1, a)} = W_{(a, -1)}$ , and  $W = W_{(1, b)} = U_{(b, -1)}$ .

$\mathbb{S}$	id	$s$	$e$	$es$
$id$	$xy + b(a(x)y)$	$xy + a(b(x)y)$	$xy + b(\hat{a}(x)y)$	$xy + \hat{b}(\hat{a}(x)y)$
$t$	$xy + \hat{a}(\hat{b}(x)y)$	$xy + \hat{a}(b(x)y)$	$xy + a(\hat{b}(x)y)$	$xy + \hat{b}(a(x)y)$
$d$	$xy + b(xa(y))$	$xy + a(xb(y))$	$xy + b(x\hat{a}(y))$	$xy + \hat{a}(xb(y))$
$td$	$xy + \hat{a}(x\hat{b}(y))$	$xy + \hat{b}(x\hat{a}(y))$	$xy + a(x\hat{b}(y))$	$xy + \hat{b}(xa(y))$
$dt$	$xy + \hat{b}(x)a(y)$	$xy + \hat{a}(x)b(y)$	$xy + \hat{b}(x)\hat{a}(y)$	$xy + a(x)b(y)$
$dtd$	$xy + a(x)\hat{b}(y)$	$xy + b(x)\hat{a}(y)$	$xy + \hat{a}(x)\hat{b}(y)$	$xy + b(x)a(y)$

Here the element in the top row is applied first, e.g. the multiplication in the third row, second column corresponds to  $(S(U, W)^s)^d$ . Note that  $(S(U, W)^d)^s$  is undefined, as  $s$  (and  $e$ ) are only defined on BEL-configurations. To incorporate  $d$  to form a single group action, we would require a way to find  $(U', W')$  such that  $S(U', W') \simeq S(U, W)^d$ . As yet we have no such method.

**Example 3.** Let  $b(x) = -x^\beta$ ,  $a(x) = c^{1/\beta}x^{\alpha/\beta}$ .

$\mathbb{S}$	id	$s$	$e$	$es$
$id$	$(c, \alpha, \beta)$	$(c^{1/\beta}, \alpha, \alpha/\beta)$	$(c^{\beta/\alpha}, \beta^2/\alpha, \beta)$	$(c^{1/\alpha}, \beta^2/\alpha, \beta/\alpha)$
$t$	$(c^{1/\alpha}, 1/\alpha, \beta/\alpha)$	$(c^{1/\alpha\beta}, 1/\alpha, 1/\beta)$	$(c^{1/\beta}, \alpha/\beta^2, \alpha/\beta)$	$(c^{1/\beta^2}, \alpha/\beta^2, 1/\beta)$

Comparing this table with Theorem 1, it is not difficult to see that  $(c, \alpha, \beta)$  can be chosen such that these 8 presemifields are pairwise non-isotopic. Furthermore, calculating the full Knuth orbits as in Example 1, we see that these operations can indeed produce 24 different isotopy classes from a single BEL-configuration.

## 6 Rank two semifields

Rank two semifields, that is, semifields which are two dimensional over a nucleus have received particular focus in recent years, due to their close connections to various objects in finite geometry. See for example [15], Section 3 for an overview.

Suppose  $n = 2m$  is even, and suppose  $\mathbb{S}$  is two dimensional over its right nucleus. Then we can assume

$$\mathbb{S}(x, y) = f_1(x)y - (f_2(x)y)^{q^m}$$

for some endomorphisms  $f_1, f_2$ . Then  $\mathbb{S} = \mathbb{S}_{f,g}$ , where  $g = (1, x \mapsto -x^{q^m})$ . Hence every rank two semifield is of the form  $\mathbb{S}_{f,g}$  for some  $f$ , and so can be constructed from a BEL-configuration  $(\mathcal{D}, U_f, W_g)$  in  $V(2n, q)$ . In this case,  $\text{im}(\psi_g) = \text{End}_{\mathbb{F}_{q^m}}(\mathbb{F}_{q^n})$ , and  $\psi_g(\tilde{\mathcal{B}}(W_g))$  is precisely the set of singular  $\mathbb{F}_{q^m}$ -endomorphisms of  $\mathbb{F}_{q^n}$ , and corresponds to a hyperbolic quadric in a projective 3-dimensional space over  $\mathbb{F}_{q^m}$ .

Hence classifying BEL-configurations  $(\mathcal{D}, U, W_g)$  in this case is precisely the same as classifying linear sets of rank  $n$  skew from a hyperbolic quadric in  $\text{PG}(3, q^m)$ . This is the approach used in for example [5], [7], [19], [6] to classify rank two semifields of dimension 4 and 6 over their centre.

So, as was shown in [3], the switching operation can be applied to rank two semifields. In [11], it was shown that in this special case, switching has a geometric interpretation (“dualising an ovoid”). In [9] it was shown that in this case, switching is well defined up to isotopism. In [2] it was shown that this operation is, in general, non-trivial. In [18] this operation was christened the translation dual.

Now we show that the operation  $e$  defined in Section 5.2 turns out to be trivial in this case. For the case  $W = W_{(1, x \mapsto x^{q^m})}$ , we have that  $W^\epsilon = W$ . For let  $u, v \in W$ . Then there exist  $x, y \in \mathbb{F}_{q^n}$  such that  $u = (x, x^{q^m})$ ,  $v = (y, y^{q^m})$ . Then

$$\begin{aligned} b_\epsilon(u, v) &= \text{tr}(xy^{q^m} - x^{q^m}y) \\ &= \text{tr}(xy^{q^m}) - \text{tr}(xy^{q^{n-m}}) \\ &= 0, \end{aligned}$$

since  $n = 2m$ . Hence when  $W = W_{(1, x \mapsto -x^{q^m})}$ ,

$$[U, W]^\epsilon = [U, W^\epsilon] = [U, W],$$

implying that the operation  $e$  is trivial in the case of rank two semifields. However, as seen in Section 5.2, this operation is not always trivial.

## References

- [1] Albert A.A.; *Finite division algebras and finite planes*. In: Proceedings of Symposia in Applied Mathematics, vol. 10, 53–70. American Mathematical Society, Providence (1960).
- [2] Ball, S., Brown, M. R.; *The six semifield planes associated with a semifield flock*, Adv. Math. 189 (2004), 68-87.
- [3] Ball, S., Ebert, G., Lavrauw, M.; *A geometric construction of finite semifields*, J. Algebra 311 (2007), 117-129.
- [4] Biliotti, M., Jha, V., Johnson, N. L.; *The collineation groups of generalized twisted field planes*, Geom. Dedicata 76 (1999), 97-126.
- [5] Cardinali, I., Polverino, O., Trombetti, R.; *Semifield planes of order  $q^4$  with kernel  $F_{q^2}$  and center  $F_q$* , European J. Combin. 27 (2006), 940-961.
- [6] Ebert, G.L., Marino, G., Polverino, O., Trombetti, R.; *On the multiplication of some semifields of order  $q^6$* , Finite Fields Appl. 15 (2009), 160-173.
- [7] Johnson, N.L., Marino, G., Polverino, O., Trombetti, R.; *Semifields of order  $q^6$  with left nucleus  $F_{q^3}$  and center  $F_q$* , Finite Fields Appl. 14 (2008), 456-469.
- [8] Kantor, W. M.; *Finite semifields*, Finite geometries, groups, and computation, 103-114, Walter de Gruyter GmbH & Co. KG, Berlin, 2006.
- [9] Kantor, W. M., *HMO-planes*, Adv. Geom. 9 (2009), 31-43.
- [10] Knuth, D. E.; *Finite semifields and projective planes*. J. Algebra 2 (1965) 182-217.
- [11] Lavrauw, M.; *The two sets of three semifields associated with a semifield flock*, Innov. Incidence Geom. 2 (2005), 101-107.
- [12] Lavrauw, M.; *On the isotopism classes of finite semifields*, Finite Fields Appl. 14 (2008), 897-910.
- [13] Lavrauw, M.; *Finite semifields with a large nucleus and higher secant varieties to Segre varieties*, Adv. Geom. 11 (2011), 399-410.
- [14] Lavrauw, M.; *Finite semifields and nonsingular tensors*, Des. Codes Cryptogr. 68, Issue 1-3, (2013), 205–227
- [15] Lavrauw, M., Polverino, O.; *Finite semifields*. Chapter in *Current research topics in Galois Geometry* (Editors J. De Beule and L. Storme), NOVA Academic Publishers, New York, 2011.



- [16] Lavrauw, M., Sheekey, J., Zanella, C.; *On embeddings of minimum dimension of  $\text{PG}(n, q) \times \text{PG}(n, q)$* , Des. Codes Cryptogr., Published online August 2013.
- [17] Lavrauw, M., Van de Voorde, G.; *Field reduction and linear sets in finite geometry*, preprint arXiv:1310.8522v1.
- [18] Lunardon, G., Marino, G., Polverino, O., Trombetti, R.; *Translation dual of a semifield*, J. Combin. Theory Ser. A 115 (2008), 1321-1332.
- [19] Marino, G., Polverino, O., Trombetti, R.; *On  $\mathbb{F}_q$ -linear sets of  $\text{PG}(3, q^3)$  and semifields*, J. Combin. Theory Ser. A 114 (2007), 769-788.